McAfee

personalfirewallplus

Guia do Usuário

COPYRIGHT

ATRIBUIÇÕES DE MARCAS COMERCIAIS

INFORMAÇÕES SOBRE LICENÇA

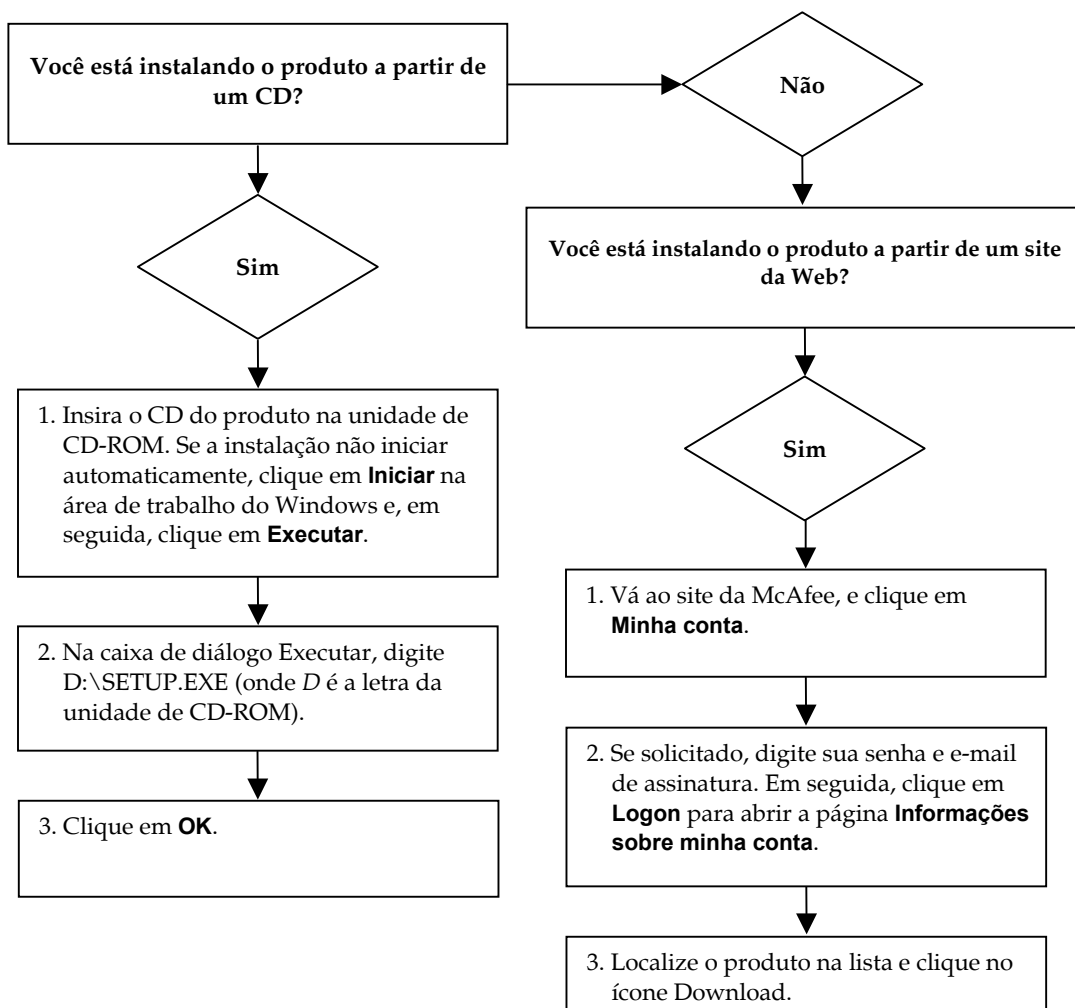
Contrato de licença

AVISO A TODOS OS USUÁRIOS: LEIA ATENTAMENTE O CONTRATO LEGAL CORRESPONDENTE À LICENÇA POR VOCÊ ADQUIRIDA. NELE ESTÃO DEFINIDOS OS TERMOS E AS CONDIÇÕES GERAIS PARA A UTILIZAÇÃO DO SOFTWARE LICENCIADO. CASO NÃO SAIBA O TIPO DE LICENÇA QUE VOCÊ ADQUIRIU, CONSULTE A DOCUMENTAÇÃO RELACIONADA À COMPRA E VENDA OU À CONCESSÃO DE LICENÇA, INCLUÍDA NO PACOTE DO SOFTWARE OU FORNECIDA SEPARADAMENTE (COMO UM LIVRETO, UM ARQUIVO NO CD DO PRODUTO OU UM ARQUIVO DISPONÍVEL NO SITE DA WEB EM QUE O PACOTE DE SOFTWARE FOI OBTIDO POR DOWNLOAD). SE NÃO CONCORDAR COM TODOS OS TERMOS ESTABELECIDOS NO CONTRATO, NÃO INSTALE O SOFTWARE. SE FOR APLICÁVEL, VOCÊ PODE DEVOLVER O PRODUTO PARA A MCAFEE, INC. OU PARA O LOCAL ONDE ADQUIRIU O PRDUTO, A FIM DE OBTER O REEMBOLSO TOTAL.

Atribuições

Este produto inclui ou pode incluir:
♦ Software desenvolvido pelo OpenSSL Project para uso no OpenSSL Toolkit (http://www.openssl.org/). ♦ Software de criptografia criado por Eric A. Young e software criado por Tim J. Hudson. ♦ Alguns programas de software que estão licenciados (ou sublicenciados) ao usuário de acordo com a GNU General Public License (GPL) ou com outras licenças de Software livre que, entre outros direitos, permitem que os usuários copiem, modifiquem ou redistribuam determinados programas, ou partes deles, e também tenham acesso ao código fonte. A GPL requer, para qualquer um desses softwares licenciados e distribuídos em formato binário executável, que o código fonte seja disponibilizado a esses usuários. O código fonte de qualquer um desses softwares licenciados sob a GPL está disponível neste CD. Se alguma licença de Software livre exigir que a McAfee, Inc. conceda direitos de uso, de cópia ou de modificação de um programa de software mais abrangentes que os direitos concedidos neste acordo, estes últimos terão precedência sobre as restrições e os direitos mencionados neste documento. ♦ Software criado originalmente por Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software criado originalmente por Robert Nordier, Copyright © 1996-7 Robert Nordier. ♦ Software criado por Douglas W. Sauder. ♦ Software desenvolvido pela Apache Software Foundation (http://www.apache.org/). Uma cópia do contrato de licença deste software pode ser encontrada em www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation e outros. ♦ Software desenvolvido pela CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. ♦ FEAD® Tecnologia Optimizer®, copyright Netopsystems AG, Berlim, Alemanha. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. e/ou Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software com copyright da Thai Open Source Software Center Ltd. e Clark Cooper, © 1998, 1999, 2000. ♦ Software com copyright dos mantenedores da Expat. ♦ Software com copyright da The Regents of the University of California, © 1989. ♦ Software com copyright de Gunnar Ritter. ♦ Software com copyright da Sun Microsystems®, Inc.© 2003. ♦ Software com copyright de Gisle Aas. © 1995-2003. ♦ Software com copyright de Michael A. Chase, © 1999-2000. ♦ Software com copyright de Neil Winton, © 1995-1996. ♦ Software com copyright da RSA Data Security, Inc., © 1990-1992. ♦ Software com copyright de Sean M. Burke, © 1999, 2000. ♦ Software com copyright de Martijn Koster, © 1995. ♦ Software com copyright de Brad Appleton, © 1996-1999. ♦ Software com copyright de Michael G. Schwern, © 2001. ♦ Software com copyright de Graham Barr, © 1998. ♦ Software com copyright de Larry Wall e Clark Cooper, © 1998-2000. ♦ Software com copyright de Frodo Looijaard, © 1997. ♦ Software com copyright da Python Software Foundation, Copyright © 2001, 2002, 2003. Uma cópia do contrato de licença deste software pode ser encontrada em www.python.org. ♦ Software com copyright de Beman Dawes, © 1994-1999, 2002. ♦ Software criado por Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software com copyright de Simone Bordet e Marco Cravero, © 2002. ♦ Software com copyright de Stephen Purcell, © 2001. ♦ Software desenvolvido pela Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). ♦ Software com copyright da International Business Machines Corporation e outros, © 1995-2003. ♦ Software desenvolvido pela University of California, Berkeley e seus colaboradores. ♦ Software desenvolvido por Ralf S. Engelschall <rse@engelschall.com> para uso no projeto mod_ssl (http://www.modssl.org/). ♦ Software com copyright de Kevlin Henney, © 2000-2002. ♦ Software com copyright de Peter Dimov e Multi Media Ltd. © 2001, 2002. ♦ Software com copyright de David Abrahams, © 2001, 2002. Consulte http://www.boost.org/libs/bind/bind.html para obter a documentação. ♦ Software com copyright de Steve Cleary, Beman Dawes, Howard Hinnant e John Maddock, © 2000. ♦ Software com copyright de Boost.org, © 1999-2002. ♦ Software com copyright de Nicolai M. Josuttis, © 1999. ♦ Software com copyright de Jeremy Siek, © 1999-2001. ♦ Software com copyright de Daryle Walker, © 2001. ♦ Software com copyright de Chuck Allison e Jeremy Siek, © 2001, 2002. ♦ Software com copyright de Samuel Krempp, © 2001. Consulte http://www.boost.org para obter atualização, documentação e histórico da revisão. ♦ Software com copyright de Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software com copyright da Cadenza New Zealand Ltd., © 2000. ♦ Software com copyright de Jens Maurer, © 2000, 2001. ♦ Software com copyright de Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software com copyright de Ronald Garcia, © 2002. ♦ Software com copyright de David Abrahams, Jeremy Siek, e Daryle Walker, © 1999-2001. ♦ Software com copyright de Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software com copyright de Housemarque Oy <http://www.housemarque.com>, © 2001. ♦ Software com copyright de Paul Moore, © 1999. ♦ Software com copyright de Dr. John Maddock, © 1998-2002. ♦ Software com copyright de Greg Colvin e Beman Dawes, © 1998, 1999. ♦ Software com copyright de Peter Dimov, © 2001, 2002. ♦ Software com copyright de Jeremy Siek e John R. Bandela, © 2001. ♦ Software com copyright de Joerg Walter e Mathias Koch, © 2000-2002.

Cartão de início rápido

Se estiver instalando o produto a partir de um CD ou de um site da Web, imprima esta página de referência para sua conveniência.

Para obter mais informações

Para ver os Guias do Usuário no CD do produto, verifique se Acrobat Reader está instalado; do contrário, instale-o agora a partir do CD de produto da McAfee.

1. Instale o CD do produto na unidade de CD-ROM.
2. Abra o Windows Explorer: Clique em **Iniciar** na área de trabalho do Windows e, em seguida, em **Pesquisar**.
3. Localize a pasta Manuais e clique duas vezes no arquivo .PDF do Guia do Usuário a ser aberto.

Benefícios do registro

A McAfee recomenda que você siga as etapas simples indicadas no produto para nos transmitir o seu registro diretamente. O registro garante que você receba assistência técnica conveniente e confiável, além dos seguintes benefícios:

- Suporte eletrônico GRATUITO.
- Atualizações de arquivos de atualização com definição dos vírus (.DAT) por um ano após a instalação quando você adquire o software VirusScan.

  Vá para http://www.mcafee.com/ para obter o preço de um ano adicional das assinaturas de vírus.
- Garantia de 60 dias, que cobre a substituição do CD do software se ele apresentar defeitos ou se estiver danificado.
- Atualização do filtro SpamKiller por um ano após a instalação, quando o software SpamKiller é adquirido.

  Vá para http://www.mcafee.com/ para obter o preço de um ano adicional de atualizações do filtro.
- Atualização do pacote McAfee Internet Security por um ano após a instalação quando o software MIS é adquirido.

  Vá até http://www.mcafee.com/ para obter o preço de um ano adicional de atualizações do conteúdo.

Suporte técnico

Para obter suporte técnico, visite http://www.mcafeehelp.com/.

Nosso site de suporte oferece acesso ininterrupto ao Assistente de respostas de fácil utilização, a fim de obter soluções para as questões de suporte mais comuns.

Os usuários mais experientes também podem experimentar as opções avançadas, que incluem uma pesquisa de palavra-chave e nossa árvore de ajuda. Se a solução não for encontrada, é possível acessar as opções GRATUITAS do Chat Now! e do E-mail Express!. O Chat e o e-mail ajudam a contatar os engenheiros de suporte qualificados de forma rápida pela Internet, sem custo nenhum. Como alternativa, você pode obter informações do suporte telefônico em http://www.mcafeehelp.com/.

Conteúdo

Introdução 1

Bem-vindo ao McAfee Personal Firewall Plus.

O software McAfee Personal Firewall Plus oferece proteção avançada para seu computador e seus dados pessoais. O Personal Firewall estabelece uma barreira entre o seu computador e a Internet, monitorando de forma silenciosa o tráfego da Internet em busca de atividades suspeitas.

Com ele, são obtidos os seguintes recursos:

- Defesa contra possíveis sondagens e ataques de hackers
- Defesas antivírus adicionais
- Monitoramento da atividade da rede e da Internet
- Alerta sobre eventos potencialmente hostis
- Informações detalhadas sobre tráfego suspeito na Internet
- Integração da funcionalidade Hackerwatch.org, incluindo a geração de relatórios de eventos, ferramentas de autoteste e o recurso de envio de eventos relatados por e-mail para outras autoridades on-line
- Recursos detalhados de rastreamento e pesquisa de eventos

Novos recursos

- **Suporte aprimorado a jogos**
  O McAfee Personal Firewall Plus protege o computador contra tentativas de invasão e atividades suspeitas durante jogos de tela cheia, mas pode ocultar alertas se detectar tentativas de invasão ou atividades suspeitas. Os alertas vermelhos são exibidos depois que você sair do jogo
- **Manipulação aprimorada de acesso**
  O McAfee Personal Firewall Plus permite que os usuários concedam dinamicamente aos aplicativos acesso temporário à Internet. O acesso é restrito ao tempo decorrido entre a inicialização e o encerramento do aplicativo. Quando o Personal Firewall detecta um programa desconhecido tentando comunicação com a Internet, um alerta vermelho oferece a opção de conceder ao aplicativo o acesso temporário à Internet.

- **Controle de segurança aprimorado**
  A execução do recurso de Bloqueio do McAfee Personal Firewall Plus permite bloquear momentaneamente todo o tráfego de entrada e saída da Internet entre o computador e a Internet. Os usuários podem ativar e desativar o Bloqueio de três locais no Personal Firewall.

- **Opções aprimoradas de recuperação**
  É possível executar as Opções de redefinição para restaurar automaticamente as configurações padrão do Personal Firewall. Se o Personal Firewall exibir um comportamento insatisfatório que não possa ser corrigido, é possível desfazer as configurações atuais e retornar às configurações padrão do produto.

- **Proteção à conectividade com a Internet**
  Para evitar que um usuário inadvertidamente desabilite sua própria conexão com a Internet, a opção de proibir um endereço da Internet é excluída em um alerta azul quando o Personal Firewall detecta uma conexão da Internet originada de um servidor DHCP ou DNS. Se o tráfego de entrada não for proveniente de um servidor DHCP ou DNS, a opção será exibida.

- **Integração aprimorada com o HackerWatch.org**
  A notificação de possíveis hackers agora ficou mais fácil. O McAfee Personal Firewall Plus aprimora a funcionalidade do HackerWatch.org, que inclui o envio de eventos potencialmente mal-intencionados para o banco de dados.

- **Manipulação estendida inteligente de aplicativos**
  Quando um aplicativo busca acesso à Internet, o Personal Firewall primeiro verifica se ele reconhece o aplicativo como confiável ou mal-intencionado. Se o aplicativo for reconhecido como confiável, o Personal Firewall permitirá automaticamente o acesso à Internet para que você não precise fazê-lo.

- **Detecção avançada de cavalos de Tróia**
  O McAfee Personal Firewall Plus combina o gerenciamento de conexão de aplicativos com um banco de dados avançado para detectar e impedir que aplicativos potencialmente mal-intencionados, como cavalos de Tróia, acessem a Internet e transmitam seus dados pessoais.

- **Rastreamento visual aprimorado**
  O rastreamento visual inclui mapas gráficos de fácil leitura, que mostram a origem de tráfego e de ataques hostis em todo o mundo, inclusive informações detalhadas sobre contatos/proprietários de endereços IP de origem.

- **Mais fácil de usar**
  O McAfee Personal Firewall Plus inclui um Assistente de configuração e um Tutorial para ajudar o usuário a configurar e usar o firewall. Embora o produto tenha sido criado para ser usado sem intervenção, a McAfee oferece aos usuários vários recursos para que eles entendam e apreciem o que o firewall tem a oferecer.

- **Detecção aprimorada de invasões**
  O Sistema de detecção de invasão (IDS) do Personal Firewall detecta padrões de ataques comuns e outras atividades suspeitas. A detecção de invasões monitora todos os pacotes de dados em busca de transferências de dados ou métodos de transferência suspeitos e os registra no registro de eventos.

- **Análise avançada de tráfego**
  O McAfee Personal Firewall Plus oferece aos usuários uma visão dos dados que entram e saem de seus computadores e exibe conexões de aplicativos, incluindo aqueles que estão ativamente "na escuta" em busca de conexões abertas. Isso permite que os usuários vejam e combatam aplicativos que possam estar propensos à invasão.

Requisitos do sistema

- Microsoft® Windows 98, Windows Me, Windows 2000 ou Windows XP
- PC com processador compatível com o Pentium
  Windows 98, 2000: 133 MHz ou superior
  Windows Me: 150 MHz ou superior
  Windows XP (Home e Pro): 300 MHz ou superior
- RAM
  Windows 98, Me, 2000: 64 MB
  Windows XP (Home e Pro): 128 MB
- 40 MB de espaço em disco rígido
- Microsoft® Internet Explorer 5.5 ou posterior

NOTA
Para atualizar para a versão mais recente do Internet Explorer, visite o site da Microsoft em http://www.microsoft.com/.

Desinstalando outros firewalls

Antes de instalar o software do McAfee Personal Firewall Plus, é necessário desinstalar todos os demais programas de firewall do computador. Siga as instruções de desinstalação do programa de firewall para executar esse procedimento.

NOTA
Se você usa o Windows XP, não é necessário desativar o recurso incorporado de firewall antes de instalar o McAfee Personal Firewall Plus. Mas, mesmo assim, recomendamos que você o desative. Do contrário, você não receberá eventos no registro de Eventos de entrada no McAfee Personal Firewall Plus.

Definindo o firewall padrão

O McAfee Personal Firewall é capaz de gerenciar permissões e o tráfego de aplicativos da Internet em seu computador, mesmo que o Windows Firewall esteja sendo executado.

Quando instalado, o McAfee Personal Firewall desativa automaticamente o Windows Firewall e se define como o firewall padrão. Assim, você receberá apenas a funcionalidade e as mensagens do McAfee Personal Firewall. Se, depois disso, você ativar o Windows Firewall no centro de segurança ou no painel de controle do Windows, permitindo que os dois firewalls sejam executados no computador, isso poderá resultar em perda parcial de dados no registro do Firewall, bem como em mensagens duplicadas de status e de alerta.

NOTA

Se os dois firewalls estiverem ativados, o McAfee Personal Firewall não mostrará todos os endereços IP bloqueados na guia Eventos de entrada. O Windows Firewall intercepta e bloqueia a maioria desses eventos, evitando que o McAfee Personal Firewall os detecte e os registre. Entretanto, o McAfee Personal Firewall pode bloquear o tráfego adicional com base em outros fatores de segurança, e esse tráfego será registrado.

Por padrão, o registro é desativado no Windows Firewall. No entanto, para manter os dois firewalls ativados, é possível ativar o registro do Windows Firewall. O registro padrão do Windows Firewall é C:\Windows\pfirewall.log

Para assegurar que o computador estará protegido por ao menos um firewall, o Windows Firewall é reativado automaticamente quando o McAfee Personal Firewall é desinstalado.

Se você desativar o McAfee Personal Firewall ou definir o nível de segurança como **Aberto** sem ativar manualmente o Windows Firewall, toda a proteção de firewall será removida, com exceção dos aplicativos bloqueados anteriormente.

Definindo o nível de segurança

Você pode configurar opções de segurança para indicar como o Personal Firewall reagirá quando detectar um tráfego indesejado. Por padrão, o nível de segurança **Padrão** é ativado. No nível de segurança **Padrão**, quando um aplicativo solicita acesso à Internet e você o concede, está fornecendo acesso total ao aplicativo. O acesso total permite que o aplicativo envie e receba dados não solicitados em portas que não sejam do sistema.

Para definir as configurações de segurança:

1 Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Opções**.

2 Clique no ícone **Configurações de segurança**.

3 Defina o nível de segurança movendo o botão deslizante para o nível desejado.

   O nível de segurança varia de Bloqueado a Aberto:

   - **Bloqueado —** Todas as conexões da Internet no computador estão fechadas. Use esta configuração para bloquear as portas configuradas como abertas na página Serviços do sistema.

   - **Segurança rígida —** Quando um aplicativo solicita um tipo específico de acesso à Internet (por exemplo, Somente acesso de saída), é possível permitir ou proibir ao aplicativo a conexão à Internet. Se o aplicativo solicitar posteriormente o Acesso total, poderá conceder Acesso total ou limitá-lo a Somente acesso de saída.

   - **Segurança padrão (recomendada) —** Quando um aplicativo solicita e recebe acesso à Internet, ele recebe acesso total à Internet para manipular o tráfico de entrada e de saída.

   - **Segurança confiável —** Todos os aplicativos são considerados confiáveis quando tentam acessar a Internet pela primeira vez. No entanto, é possível configurar o Personal Firewall para usar alertas que notifiquem sobre novos aplicativos no computador. Use esta configuração caso desconfie que alguns jogos ou arquivos de mídia não estejam funcionando.

   - **Aberto —** O firewall é desativado. Essa configuração permite que todo o tráfego passe pelo Personal Firewall sem filtro.

     NOTA
     Os aplicativos bloqueados anteriormente continuarão bloqueados se o firewall estiver definido como **Aberto** ou **Bloqueado**. Para evitar que isso ocorra, altere as permissões do aplicativo para **Permitir acesso total** ou exclua a regra de permissão **Bloqueado** da lista **Aplicativos da Internet**.

4 Selecione configurações adicionais de segurança:

   NOTA
   Se o computador for executado no Windows XP e vários usuários do XP tiverem sido adicionados, essas opções estarão disponíveis somente se você tiver efetuado logon como administrador.

- **Gravar os eventos da detecção de invasão (IDS) no registro de Eventos de entrada —** Se esta opção for selecionada, os eventos detectados pelo IDS serão exibidos no registro de Eventos de entrada. O Sistema de detecção de invasão (IDS) detecta tipos comuns de ataques e outras atividades suspeitas. A detecção de invasão monitora todos os pacotes de dados de entrada e de saída em busca de métodos de transferência ou transferências de dados suspeitos. Ela compara esses dados com um banco de dados de "assinaturas" e rejeita automaticamente os pacotes vindos de computadores ofensivos.

  O IDS procura padrões de tráfego específicos usados pelos invasores. A detecção também verifica todos os pacotes recebidos pelo computador para detectar o tráfego de ataques suspeitos ou conhecidos. Por exemplo, se o Personal Firewall encontra pacotes ICMP, ele os analisa em busca de padrões de tráfegos suspeitos, comparando o tráfego ICMP com padrões de ataques conhecidos.

- **Aceitar pedidos de ping ICMP** — O tráfego ICMP é usado principalmente para executar rastreamentos e pings. O recurso de ping normalmente é usado para executar um teste rápido antes de estabelecer comunicações. Se você estiver usando ou já tiver usado um programa de compartilhamento de arquivos ponto a ponto, talvez receba muitas solicitações de ping. Se esta opção for selecionada, o Personal Firewall permitirá todas as solicitações de ping sem incluí-las no registro de Eventos de entrada. Se você deixar esta opção desmarcada, o Personal Firewall bloqueará todas as solicitações de ping e as incluirá no registro de Eventos de entrada.

- **Permitir que usuários restritos alterem as configurações do Personal firewall** — Se o computador estiver executando o Windows XP ou o Windows 2000 Professional com vários usuários, selecione essa opção para permitir a usuários restritos do XP a modificação das configurações do Personal Firewall.

5. Clique em **OK** ao terminar de fazer as alterações.

Testando o McAfee Personal Firewall Plus

É possível testar a instalação do Personal Firewall para verificar possíveis vulnerabilidades a atividades suspeitas e invasões.

Para testar a instalação do Personal Firewall usando o ícone da McAfee na bandeja do sistema:

- Clique com o botão direito do mouse no ícone da McAfee, na bandeja de sistema do Windows e selecione **Testar o firewall**.

O Personal Firewall abre o Internet Explorer e acessa http://www.hackerwatch.org/, um site da Web mantido pela McAfee. Siga as instruções na página Hackerwatch.org Probe para testar o Personal Firewall.

Usando o McAfee SecurityCenter

O McAfee SecurityCenter é a central de produtos de segurança, que pode ser acessada pelo seu ícone na bandeja de sistema do Windows ou na área de trabalho do Windows. Com ele, é possível executar estas tarefas úteis:

- Obter uma análise gratuita de segurança no computador.
- Inicializar, gerenciar e configurar todas as suas assinaturas da McAfee a partir de um ícone.
- Exibir alertas de vírus atualizados continuamente e as informações mais recentes sobre produtos.
- Obter links rápidos para as perguntas freqüentes e detalhes da conta no site da McAfee.

NOTA
Para obter mais informações sobre os recursos, clique em **Ajuda** na caixa de diálogo **SecurityCenter**.

Enquanto o SecurityCenter estiver em execução e todos os recursos da McAfee instalados no computador estiverem ativos, um ícone M vermelho será exibido na bandeja de sistema do Windows. Essa área geralmente encontra-se no canto direito inferior da área de trabalho do Windows e contém o relógio.

Se um ou mais aplicativos da McAfee instalados no computador estiverem desativados, o ícone da McAfee se tornará preto .

Para iniciar o McAfee SecurityCenter:

1. Clique com o botão direito do mouse no ícone da McAfee e selecione **Abrir o Security Center**.

Para iniciar o Personal Firewall no McAfee SecurityCenter:

1. No SecurityCenter, clique na guia **Personal Firewall Plus**.
2. Selecione uma tarefa no menu Desejo.

Para iniciar o Personal Firewall no Windows:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja do sistema do Windows e, em seguida, aponte para **Personal Firewall**.
2. Selecione uma tarefa.

Usando o McAfee Personal Firewall Plus

2

Para abrir o Personal Firewall:

- Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione uma tarefa.

Sobre a página Resumo

O Resumo do Personal Firewall contém quatro páginas:

- Resumo principal
- Resumo do aplicativo
- Resumo de eventos
- Resumo do HackerWatch

As páginas de resumo contêm vários relatórios sobre eventos de entrada recentes, status de aplicativos e a atividade de invasão mundial relatada pelo HackerWatch.org. Também é possível encontrar links para tarefas comuns executadas no Personal Firewall.

Para abrir a página Resumo principal no Personal Firewall:

- Clique com o botão direito do mouse no ícone da McAfee, na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo** (Figura 2-1).

Figura 2-1. Página Resumo principal

Clique nestas opções para navegar para outras páginas de resumo:

Item	Descrição
Alterar exibição	Clique em **Alterar exibição** para abrir uma lista das páginas de resumo. Na lista, selecione uma página do Resumo para ser exibida.
Seta para a direita	Clique no ícone de seta para a direita para exibir a próxima página Resumo.
Seta para a esquerda	Clique no ícone de seta para a esquerda a fim de exibir a página de resumo anterior.
Principal	Clique neste ícone para retornar à página **Resumo principal**.

A página Resumo principal fornece as seguintes informações:

Item	Descrição
Configuração de segurança	O status da configuração de segurança indica o nível de segurança para o qual o firewall está definido. Clique no link para alterar o nível de segurança.
Eventos bloqueados	O status dos eventos bloqueados exibe o número de eventos que foram bloqueados no dia. Clique no link para ver detalhes do evento na página Eventos de entrada.
Alterações na regra do aplicativo	O status da regra do aplicativo mostra o número de regras de aplicativo que foram alteradas recentemente. Clique no link para exibir a lista de aplicativos permitidos e bloqueados e para modificar permissões de aplicativos.
O que há de novo?	**O que há de novo?** mostra o último aplicativo que recebeu acesso total à Internet.
Último evento	**Último evento** esta opção mostra os eventos de entrada mais recentes. Você pode clicar em um link para rastrear um evento ou para confiar no endereço IP. A confiança em um endereço IP permite que todo o tráfego vindo desse endereço acesse o seu computador.
Relatório diário	**Relatório diário** exibe o número de eventos de entrada que o Personal Firewall bloqueou no dia, na semana e no mês. Clique no link para exibir detalhes do evento na página Eventos de entrada.
Aplicativos ativos	**Aplicativos ativos** exibe os aplicativos que estão em execução no computador e acessando a Internet. Clique em um aplicativo para exibir os endereços IP que o aplicativo está acessando.
Tarefas comuns	Clique em um link em **Tarefas comuns** para ir até as páginas do Personal Firewall nas quais é possível exibir a atividade do firewall e executar tarefas.

Para exibir a página Resumo do aplicativo:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo.**
2. Clique em **Alterar exibição** e selecione **Resumo do aplicativo**.

A página Resumo do aplicativo fornece as seguintes informações:

Item	Descrição
Monitor de tráfego	A opção **Monitor de tráfego** mostra as conexões de entrada e saída da Internet nos últimos quinze minutos. Clique no gráfico para exibir os detalhes da monitoração do tráfego.
Aplicativos ativos	**Aplicativos ativos** mostra o uso de largura de banda dos aplicativos mais ativos do computador nas últimas 24 horas. **Aplicativo** - o aplicativo que está acessando a Internet. **%** - a porcentagem de largura de banda usada pelo aplicativo. **Permissão** - o tipo de acesso à Internet permitido ao aplicativo. **Regra criada** - quando a regra do aplicativo foi criada.
O que há de novo?	**O que há de novo?** mostra o último aplicativo que recebeu acesso total à Internet.
Aplicativos ativos	**Aplicativos ativos** exibe os aplicativos que estão em execução no computador e acessando a Internet. Clique em um aplicativo para exibir os endereços IP que o aplicativo está acessando.
Tarefas comuns	Clique em um link em **Tarefas comuns** para ir até as páginas do Personal Firewall nas quais é possível exibir o status do aplicativo e executar tarefas relacionadas ao aplicativo.

Para exibir a página Resumo de eventos:

1 Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo.**

2 Clique em **Alterar exibição** e selecione **Resumo de eventos.**

A página Resumo de eventos oferece as seguintes informações:

Item	Descrição
Comparação de portas	**Comparação de portas** mostra um gráfico de pizza das portas mais solicitadas no computador nos últimos 30 dias. Clique em um nome de porta para exibir os detalhes da página Eventos de entrada. Também é possível mover o ponteiro do mouse sobre o número da porta para exibir a descrição.
Principais infratores	**Principais infratores** mostra os endereços IP bloqueados com mais freqüência, quando o último evento de entrada ocorreu em cada endereço e o número total de eventos de entrada de cada endereço nos últimos trinta dias. Clique em um evento para exibir os detalhes na página Eventos de entrada.

Item	Descrição
Relatório diário	**Relatório diário** exibe o número de eventos de entrada que o Personal Firewall bloqueou no dia, na semana e no mês. Clique em um número para exibir os detalhes do evento no registro de Eventos de entrada.
Último evento	**Último evento** esta opção mostra os eventos de entrada mais recentes. Clique em um link para rastrear um evento ou para confiar no endereço IP. A confiança em um endereço IP permite que todo o tráfego vindo desse endereço acesse o seu computador.
Tarefas comuns	Clique em um link em **Tarefas comuns** para ir até as páginas do Personal Firewall nas quais é possível exibir os detalhes dos eventos e executar tarefas a eles relacionadas.

Para exibir a página Resumo do HackerWatch:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Exibir resumo.**
2. Clique em **Alterar exibição** e selecione **Resumo do HackerWatch.**

A página Resumo do HackerWatch fornece as seguintes informações:

Item	Descrição
Atividade mundial	**Atividade mundial** mostra um mapa-múndi que identifica as atividades bloqueadas recentemente monitoradas pelo HackerWatch.org. Clique no mapa para abrir o mapa de análise de ameaças globais no HackerWatch.org.
Rastreamento de eventos	**Rastreamento de eventos** mostra o número de eventos de entrada enviados para o HackerWatch.org.
Atividade global de porta	**Atividade global de porta** mostra as principais portas que, nos últimos 5 dias, demonstraram ser ameaças. Clique em uma porta para exibir seu número e sua descrição.
Tarefas comuns	Clique em um link em **Tarefas comuns** para ir até as páginas do HackerWatch.org nas quais é possível obter mais informações sobre a atividade de hackers no mundo todo.

Sobre a página Aplicativos da Internet

Use a página Aplicativos da Internet para exibir a lista de aplicativos permitidos e bloqueados.

Para iniciar a página Aplicativos da Internet:

- Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Aplicativos.** (Figura 2-2).

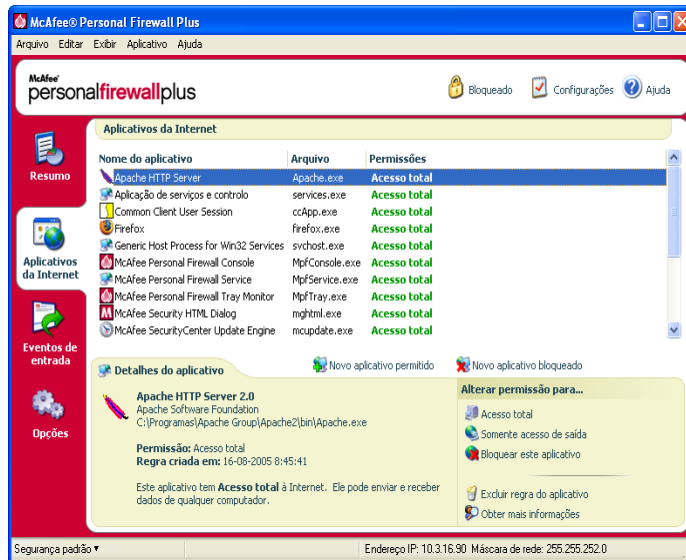



Figura 2-2. Página Aplicativos da Internet

A página Aplicativos da Internet oferece as seguintes informações:

- Nomes dos aplicativos
- Nomes dos arquivos
- Níveis de permissão atuais
- Detalhes do aplicativo: nome e versão do aplicativo, nome da empresa, nome do caminho, permissão, marcas de data e hora e explicações dos tipos de permissão.

Alterando regras de aplicativos

O Personal Firewall permite alterar o acesso às regras dos aplicativos.

Para alterar uma regra do aplicativo:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Aplicativos da Internet**.
2. Na lista **Aplicativos da Internet**, clique com o botão direito do mouse na regra de um aplicativo e selecione um nível diferente:
   - **Permitir acesso total -** permite que o aplicativo estabeleça conexões de entrada e saída da Internet.
   - **Somente acesso de saída -** permite que o aplicativo estabeleça apenas uma conexão de saída da Internet.
   - **Bloquear este aplicativo -** não permite ao aplicativo o acesso à Internet.

     NOTA
     Os aplicativos bloqueados anteriormente continuam bloqueados quando o firewall estiver configurado como **Aberto** ou **Bloqueado**. Para evitar que isso aconteça, pode-se mudar a regra de acesso do aplicativo para **Acesso total** ou excluir a regra de permissão **Bloqueado** da lista **Aplicativos da Internet**.

Para excluir uma regra do aplicativo:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Aplicativos da Internet**.
2. Na lista **Aplicativos da Internet**, clique com o botão direito do mouse na regra do aplicativo e selecione **Excluir regra do aplicativo**.

Na próxima vez que o aplicativo solicitar acesso à Internet, você poderá definir seu nível de permissão para adicioná-lo à lista novamente.

Permitindo e bloqueando os aplicativos da Internet

Para alterar a lista de aplicativos da Internet permitidos e bloqueados:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Aplicativos da Internet**.
2. Na página Aplicativos da Internet, clique em uma das seguintes opções:
   - **Novo aplicativo permitido** — permite ao aplicativo o acesso total à Internet.
   - **Novo aplicativo bloqueado** — não permite ao aplicativo o acesso à Internet.
   - **Excluir regra do aplicativo** — remove uma regra do aplicativo.

Sobre a página Eventos de entrada

Use a página Eventos de entrada para exibir o registro de Eventos de entrada gerado quando o Personal Firewall bloqueia conexões de Internet não solicitadas.

Para iniciar a página Eventos de entrada:

- Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada** (Figura 2-3).

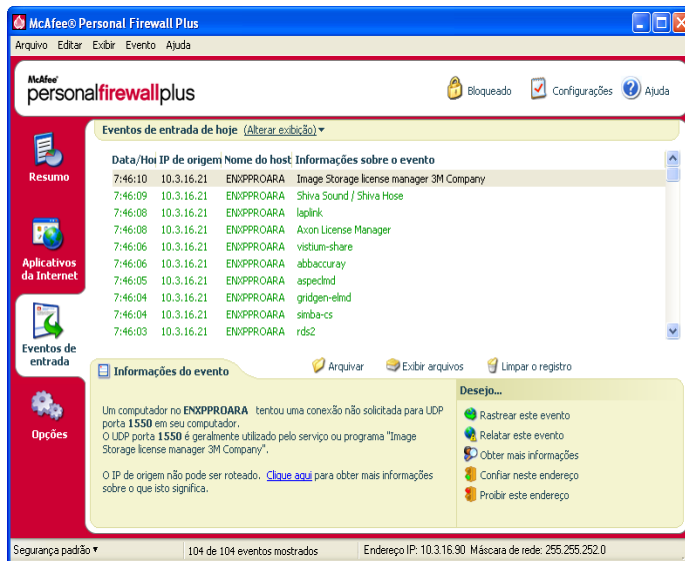



Figura 2-3. Página Eventos de entrada

A página Eventos de entrada oferece as seguintes informações:

- Marcas de data e hora
- IPs de origem
- Nomes de host
- Nomes de serviço ou de aplicativo
- Detalhes do evento: tipos de conexão, portas de conexão, IP ou nome do host e explicações de eventos de porta

Noções básicas sobre eventos

Sobre endereços IP

Os endereços IP são números: quatro números, cada um entre 0 e 255. Esses números identificam um local específico para onde o tráfego pode ser direcionado na Internet.

Tipos de endereço IP

Diversos endereços IP são incomuns por vários motivos:

Endereços IP não roteáveis — também chamados de "Espaço IP privado". Esses endereços IP não podem ser usados na Internet. Os blocos de endereços IP privados são 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.

Endereços IP de loopback — os endereços de loopback são usados para fins de teste. O tráfego enviado a esse bloco de endereços IP volta para o dispositivo que gerou o pacote. Ele nunca sai do dispositivo e é usado principalmente para teste de hardware e software. O bloco de endereços IP de loopback é 127.x.x.x.

Endereço IP nulo — é um endereço inválido. Quando detectado, o Personal Firewall indica que o tráfego utilizou um endereço IP em branco. Geralmente isso indica que o remetente está deliberadamente ocultando a origem do tráfego. O remetente não poderá receber nenhuma resposta para esse tráfego, a não ser que o pacote seja recebido por um aplicativo que reconheça o conteúdo do pacote que conterá instruções específicas desse aplicativo. Qualquer endereço que inicie com 0 (0.x.x.x) é um endereço nulo. Por exemplo, 0.0.0.0 é um endereço IP nulo.

Eventos de 0.0.0.0

Se forem exibidos eventos do endereço IP 0.0.0.0, existirão duas causas prováveis. A primeira, e mais comum, é que o computador recebeu um pacote inválido. A Internet nem sempre é 100% confiável e é comum haver pacotes com problemas. Como o Personal Firewall vê os pacotes antes que o TCP/IP possa validá-los, ele pode relatar esses pacotes como um evento.

A outra situação ocorre quando o IP de origem é fraudado ou falso. Os pacotes fraudados podem ser um sinal de que alguém está em busca de cavalos de Tróia no seu computador. O Personal Firewall bloqueia este tipo de atividade, portanto o computador está seguro.

Eventos de 127.0.0.1

Às vezes os eventos indicam o IP de origem como 127.0.0.1. Esse IP se chama endereço de loopback ou localhost.

Muitos programas legítimos usam o endereço de loopback para comunicação entre componentes. Por exemplo, é possível configurar muitos servidores de e-mail pessoal ou servidores Web por meio de uma interface da Web. Para acessar a interface, digite "http://localhost/" no navegador da Web.

O Personal Firewall permite o tráfego desses programas. Portanto, se você receber eventos de 127.0.0.1, é provável que o endereço IP de origem esteja fraudado ou seja falso. Os pacotes fraudados geralmente indicam que outro computador está em busca de cavalos de Tróia no seu computador. O Personal Firewall bloqueia essas tentativas de invasão; portanto, o computador está seguro.

Alguns programas, particularmente o Netscape 6.2 e posterior, exigem que o endereço 127.0.0.1 seja adicionado à lista de endereços IP confiáveis. Os componentes desses programas comunicam-se entre si de uma maneira que o Personal Firewall não consegue determinar se o tráfego é local ou não.

No exemplo do Netscape 6.2, se você não confiar no 127.0.0.1, não poderá usar sua lista de amigos. Portanto, se você receber tráfego de 127.0.0.1 e todos os aplicativos do computador funcionarem normalmente, é sinal de que esse tráfego pode ser bloqueado sem problemas. No entanto, se um programa (como o Netscape) tiver problemas, adicione o 127.0.0.1 à lista de endereços IP confiáveis do Personal Firewall.

Se isso resolver o problema, será necessário tomar uma decisão: se confiar no 127.0.0.1, o programa funcionará, mas você estará mais vulnerável a ataques fraudados. Se você não confiar no endereço, o programa não funcionará, mas você continuará protegido contra determinado tráfego mal-intencionado.

Eventos de computadores na LAN

Os eventos podem ser gerados por computadores da rede local (LAN). Para indicar que esses eventos são gerados pela sua rede, o Personal Firewall os exibe em verde.

Na maioria das configurações de LAN corporativas, você deve selecionar **Tornar todos os computadores da sua LAN confiáveis** nas opções de endereços IP confiáveis.

Em algumas situações, a rede "local" pode ser tão perigosa quanto a Internet, especialmente se o computador for executado em uma rede DSL de banda larga ou modem a cabo. Nesse caso, não selecione **Tornar todos os computadores da sua LAN confiáveis**. Em vez disso, adicione os endereços IP dos computadores locais à lista de endereços IP confiáveis.

Eventos de endereços IP privados

Os endereços IP de formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 são chamados de não-roteáveis ou privados. Esses endereços IP nunca devem sair da sua rede e, na maioria das vezes, são confiáveis.

O bloco 192.168 xxx.xxx é usado com o Microsoft Internet Connection Sharing (ICS). Se estiver usando ICS e receber eventos desse bloco de endereços IP, poderá adicionar o endereço IP 192.168.255.255 à lista de endereços IP confiáveis. Isso tornará todo o bloco 192.168.xxx.xxx confiável.

Se você não estiver em uma rede privada e receber eventos desses intervalos de endereços IP, talvez o endereço IP de origem esteja fraudado ou seja falso. Os pacotes fraudados geralmente são um sinal de que alguém está fazendo uma varredura em busca de cavalos de Tróia. É importante lembrar que o Personal Firewall bloqueou essa tentativa e, portanto, seu computador está seguro.

Como os endereços IP privados se referem a computadores diferentes dependendo da rede em que você está, relatar esses eventos não trará nenhum benefício. Sendo assim, não é necessário fazê-lo.

Mostrando eventos no registro de Eventos de entrada

O registro de Eventos de entrada exibe os eventos de várias formas. A exibição padrão se limita aos eventos que ocorreram no dia atual. Você também pode exibir eventos que ocorreram na semana passada ou exibir o registro completo.

O Personal Firewall também permite exibir eventos de entrada de dias específicos, de endereços da Internet específicos (endereços IP) ou eventos que contenham as mesmas informações.

Para obter informações sobre um evento, clique nele para que as informações sejam exibidas no painel **Informações sobre o evento**.

Mostrando os eventos de hoje

Use esta opção para analisar os eventos do dia.

Para mostrar os eventos de hoje:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada, e, em seguida, clique em **Mostrar eventos de hoje**.

Mostrando os eventos desta semana

Use esta opção para analisar os eventos da semana.

Para mostrar os eventos da semana:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar eventos desta semana**.

Mostrando o registro de Eventos de entrada completo

Use esta opção para analisar todos os eventos.

Para mostrar todos os eventos do registro de Eventos de entrada:

1. Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e clique em **Eventos de entrada**.
2. No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar registro completo**.

   O registro de Eventos de entrada exibe todos os eventos do registro de Eventos de entrada.

Mostrando eventos de um dia específico.

Use esta opção para analisar os eventos de um dia específico.

Para mostrar os eventos de um dia:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar somente eventos do dia selecionado**.

Mostrando eventos de um endereço da Internet específico.

Use esta opção para examinar outros eventos que se originam de um endereço da Internet específico.

Para mostrar eventos de um endereço da Internet:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e clique em **Eventos de entrada**.
2. No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar somente eventos do endereço da Internet selecionado**.

Mostrando eventos que compartilham informações idênticas.

Use esta opção para examinar outros eventos no registro de Eventos de entrada que tenham as mesmas informações do evento selecionado na coluna Informações sobre o evento. Você pode descobrir quantas vezes esse evento ocorreu e se ele é da mesma origem. A coluna Informações sobre o evento oferece uma descrição do evento e, se for conhecido, o programa ou o serviço comum que usam essa porta.

Para mostrar eventos que compartilham informações idênticas:

1 Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e clique em **Eventos de entrada**.

2 No registro de Eventos de entrada, clique com o botão direito do mouse em uma entrada e, em seguida, clique em **Mostrar somente eventos com as mesmas informações de evento**.

Respondendo a eventos de entrada

Além de analisar os detalhes sobre os eventos do registro de Eventos de entrada, é possível executar um rastreamento visual dos endereços IP de um evento desse registro ou obter detalhes do evento no site HackerWatch.org da comunidade on-line anti-hackers.

Rastreando o evento selecionado

Você pode tentar executar um rastreamento visual dos endereços IP de um evento contido no registro de Eventos de entrada.

Para rastrear um evento selecionado:

1 Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Eventos de entrada**.

2 No registro de Eventos de entrada, clique no evento a ser rastreado e, em seguida, clique em **Rastrear o evento selecionado**. Também é possível clicar duas vezes no evento para rastreá-lo.

Por padrão, o Personal Firewall inicia o rastreamento visual usando o programa Visual Trace integrado ao Personal Firewall.

Obtendo informações em HackerWatch.org

Para obter informações no HackerWatch.org:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Eventos de entrada**.

2 Selecione a entrada do evento na página Eventos de entrada e clique em **Obter mais informações** no painel **Desejo**.

O seu navegador padrão da Web é iniciado e abre o site HackerWatch.org para recuperar informações sobre o tipo de evento e saber se ele deve ser relatado.

Relatando um evento

Para relatar um evento que parece ser um ataque ao seu computador:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. Clique no evento que deseja relatar e, em seguida, clique em **Relatar este evento** no painel **Desejo**.

O Personal Firewall relata o evento para o site HackerWatch.org usando a sua ID exclusiva.

Inscrevendo-se no HackerWatch.org

Ao abrir a página Resumo pela primeira vez, o Personal Firewall contata o site HackerWatch.org para gerar a sua ID de usuário exclusiva. Se você for um usuário existente, a inscrição será validada automaticamente. Se você for um novo usuário, deverá inserir um apelido e seu endereço de e-mail e, em seguida, clicar no link de validação no e-mail de confirmação do site HackerWatch.org para poder usar os recursos de filtragem/envio de eventos por e-mail desse site.

É possível relatar eventos para o site HackerWatch.org sem validar a ID de usuário. No entanto, para filtrar eventos e enviá-los por e-mail para um amigo, é necessário inscrever-se nesse serviço.

A inscrição no serviço permite que os envios sejam rastreados e que você seja notificado se o HackerWatch.org precisar de mais informações ou de sua intervenção. A inscrição também é necessária porque precisamos confirmar todas as informações recebidas para que elas sejam úteis.

Todos os endereços de e-mail fornecidos ao site HackerWatch.org são mantidos como confidenciais. Se um ISP solicitar informações adicionais, essa solicitação será roteada através do site HackerWatch.org. Seu endereço de e-mail nunca será revelado.

Confiando em um endereço

É possível usar a página Eventos de entrada para adicionar um endereço IP à lista de endereços IP confiáveis, permitindo, assim, a conexão permanente.

Se você vir um evento na página de eventos de entrada que contenha um endereço IP em que precise confiar, faça com que o Personal Firewall sempre possibilite conexões desse endereço.

Para adicionar um endereço IP à lista de endereços IP confiáveis:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Eventos de entrada**.
2. Clique com o botão direito do mouse no evento cujo endereço IP deve ser confiável e clique em **Confiar no endereço IP de origem**.

Verifique se o endereço IP exibido na caixa de diálogo Confiar neste endereço está correto e clique em **OK**. O endereço IP será adicionado à lista de endereços IP confiáveis.

Para verificar se o endereço IP foi adicionado:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e selecione **Opções**.
2. Clique no ícone **IPs confiáveis e proibidos** e, em seguida, na guia **Endereços IP confiáveis**.

O endereço IP será exibido como verificado na lista de endereços IP confiáveis.

Proibindo um endereço

Se um endereço IP for exibido no registro de Eventos de entrada, é sinal de que o tráfego desse endereço foi bloqueado. Portanto, proibir um endereço não garante proteção adicional, a menos que as portas do computador sejam abertas deliberadamente através do recurso Serviços do sistema ou a menos que o computador tenha um aplicativo com permissão para receber tráfego.

Adicione um endereço IP à lista de endereços proibidos somente se houver uma ou mais portas que sejam deliberadamente abertas e se houver motivos para acreditar que o bloqueio seja necessário.

Se houver algum evento na página Eventos de entrada que contenha um endereço IP a ser proibido, é possível configurar o Personal Firewall para impedir sempre as conexões desse endereço.

É possível usar a página Eventos de entrada, que lista os endereços IP de todo o tráfego da Internet, para proibir um endereço IP suspeito de ser a origem de atividade suspeita ou não desejada na Internet.

Para adicionar um endereço IP à lista de endereços IP proibidos:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.

2 A página Eventos de entrada lista os endereços IP de todo o tráfego de entrada da Internet. Selecione um endereço IP e execute um dos seguintes procedimentos:

- Clique com o botão direito do mouse no endereço IP e selecione **Proibir o endereço IP de origem**.
- No menu **Desejo**, clique em **Proibir este endereço**.

3 Na caixa de diálogo Adicionar regra de endereço IP proibido, use uma ou mais de uma das configurações a seguir para determinar a regra de endereço IP proibido.

- **Endereço IP único**: O endereço IP a ser proibido. A entrada padrão é o endereço IP selecionado na página Eventos de entrada.
- **Intervalo de endereços IP**: Os endereços IP entre o endereço especificado em De endereço IP e o endereço IP especificado em Até endereço IP.
- **Fazer com que esta regra expire em**: Data e hora de expiração da regra do endereço IP proibido. Selecione os menus suspensos apropriados para selecionar a data e a hora.
- **Descrição**: Opcionalmente, descreva a nova regra.
- Clique em **OK**.

4 Na caixa de diálogo, clique em **Sim** para confirmar a configuração. Clique em **Não** para voltar à caixa de diálogo Adicionar regra de endereço IP proibido.

Se o Personal Firewall detectar um evento proveniente de uma conexão proibida da Internet, ele irá alertá-lo de acordo com o método especificado na página Configurações de alerta.

Para verificar se o endereço IP foi adicionado:

1 Clique na guia **Opções**.

2 Clique no ícone **IPs confiáveis e proibidos** e, em seguida, clique na guia **Endereços IP proibidos**.

O endereço IP é exibido como verificado na lista de endereços IP proibidos.

Gerenciando o registro de Eventos de entrada

Você pode usar a página Eventos de entrada para gerenciar os eventos do registro de Eventos de entrada gerados quando o Personal Firewall bloqueia o tráfego de Internet não solicitado.

Arquivando o registro de Eventos de entrada

É possível arquivar o registro de Eventos de entrada atual para salvar todos os eventos de entrada registrados, incluindo datas e horas, IPs de origem, nomes de host, portas e informações sobre eventos. O registro de Eventos de entrada deve ser arquivado periodicamente para impedir que fique muito grande.

Para arquivar o registro de Eventos de entrada:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. Na página Eventos de entrada, clique em **Arquivar**.
3. Na caixa de diálogo Arquivar registro, clique em **Sim** para continuar com a operação.
4. Clique em **Salvar** para salvar o arquivo no local padrão ou navegue até o local onde você deseja salvá-lo.

Nota: Por padrão, o Personal Firewall arquiva automaticamente o registro de Eventos de entrada. Marque ou desmarque **Arquivar automaticamente os eventos registrados** na página Registro de eventos para ativar ou desativar a opção.

Exibindo um registro de eventos de entrada arquivado.

Você pode exibir qualquer registro de Eventos de entrada que tenha sido arquivado anteriormente. O arquivo salvo inclui datas e horários, IPs de origem, nomes de host, portas e informações sobre eventos relacionados aos eventos.

Para exibir um registro de Eventos de entrada arquivado:

1. Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.
2. Na página Eventos de entrada, clique em **Exibir arquivos**.
3. Selecione ou procure o nome de arquivo e clique em **Abrir**.

Limpando o registro de Eventos de entrada

É possível limpar todas as informações do registro de Eventos de entrada.

AVISO: Se você limpar o registro de Eventos de entrada, ele não poderá ser recuperado. Se você acha que precisará do registro de eventos no futuro, arquive-o.

Para limpar o registro de Eventos de entrada:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Eventos de entrada**.

2 Na página Eventos de entrada, clique em **Limpar o registro**.

3 Clique em **Sim** na caixa de diálogo para limpar o registro.

Copiando um evento para a área de transferência

É possível copiar um evento para a área de transferência para poder colá-lo em um arquivo de texto usando o Bloco de notas.

Para copiar eventos para a área de transferência:

1 Clique com o botão direito do mouse no ícone da McAfee, aponte para **Personal Firewall** e selecione **Eventos de entrada**.

2 Clique com o botão direito do mouse no evento do registro de Eventos de entrada.

3 Clique em **Copiar evento selecionado para a área de transferência**.

4 Iniciar o Bloco de notas.

   - Digite `notepad` na linha de comando ou clique no botão **Iniciar** do Windows, aponte para **Programas** e, em seguida, em **Acessórios**. Selecione **Bloco de notas**.

5 Clique em **Editar** e, em seguida, clique em Colar. O texto do evento será exibido no Bloco de notas. Repita essa etapa até ter todos os eventos necessários.

6 Salve o arquivo do Bloco de notas em um local seguro.

Excluindo o evento selecionado

É possível excluir eventos do registro de Eventos de entrada.

Para excluir eventos do registro de Eventos de entrada:

1 Clique com o botão direito do mouse no ícone da McAfee na bandeja de sistema do Windows, aponte para **Personal Firewall** e, em seguida, selecione **Eventos de entrada**.

2 Clique na entrada do evento a ser excluído na página Eventos de entrada.

3 No menu Editar, clique em **Excluir evento selecionado**. O evento é excluído do registro de Eventos de entrada.

Sobre alertas

Recomendamos que você se familiarize com os tipos de alertas que encontrará ao usar o Personal Firewall. Analise os seguintes tipos de alertas que podem ser exibidos e as possíveis respostas a serem escolhidas para poder reagir com segurança a um alerta.

NOTA
As recomendações sobre alertas ajudam a decidir como lidar com o alerta. Para que as recomendações sejam exibidas nos alertas, clique na guia **Opções**, clique no ícone **Configurações de alerta** e selecione **Utilizar recomendações inteligentes** (o padrão) ou **Exibir somente as recomendações inteligentes** na lista **Recomendações inteligentes**.

Alertas vermelhos

Esses alertas contêm informações importantes que exigem atenção imediata.

- **Aplicativo de Internet bloqueado** — este alerta será exibido se o Personal Firewall impedir o acesso de um aplicativo à Internet. Por exemplo, se for exibido um alerta de programa cavalo de Tróia, a McAfee impedirá automaticamente que esse programa acesse a Internet e recomendará que se faça uma varredura do computador em busca de vírus.
- **O aplicativo deseja acessar a Internet —** este alerta é exibido quando o Personal Firewall detecta tráfego de Internet ou de rede para novos aplicativos.
- **O aplicativo foi modificado —** esse alerta é exibido quando o Personal Firewall detecta a alteração de um aplicativo ao qual havia sido concedido o acesso à Internet. Se você não tiver atualizado o aplicativo recentemente, tome cuidado ao permitir que o aplicativo modificado acesse a Internet.
- **O aplicativo solicita acesso como servidor —** esse alerta é exibido quando o Personal Firewall detecta que um aplicativo ao qual você concedeu acesso à Internet anteriormente solicitou acesso à Internet como servidor.

NOTA
A configuração padrão das Atualizações automáticas do Windows XP SP2 faz o download e instala as atualizações do sistema operacional Windows e de outros programas da Microsoft em execução no computador sem avisar o usuário. Quando um aplicativo tiver sido modificado em uma atualização silenciosa do Windows, um alerta do McAfee Personal Firewall será exibido na primeira vez em que o aplicativo Microsoft for usado após essa atualização.

IMPORTANTE
Você deve conceder acesso aos aplicativos que precisam acessar a Internet para executar atualizações de produtos on-line (como os serviços do McAfee) a fim de mantê-los atualizados.

Alerta Aplicativo da Internet bloqueado

Se for exibido um alerta de cavalo de Tróia (Figura 2-4), o Personal Firewall negará automaticamente o acesso à Internet para esse programa e recomendará que seja feita a varredura no computador em busca de vírus. Se o McAfee VirusScan não estiver instalado, inicie o McAfee SecurityCenter.

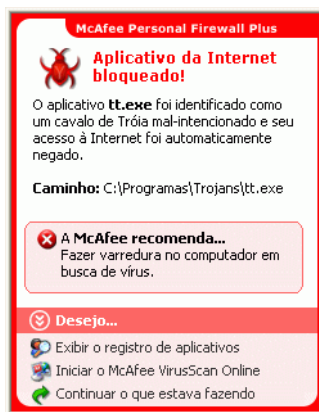



Figura 2-4. Alerta Aplicativo da Internet bloqueado

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Obter mais informações** para obter detalhes sobre o evento por meio do registro de Eventos de entrada (consulte *Sobre a página Eventos de entrada* na página 22 para saber detalhes).
- Clique em **Iniciar o McAfee VirusScan** para fazer uma varredura do computador em busca de vírus.
- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.
- Clique em **Conceder acesso de saída** para permitir uma conexão de saída (segurança **Rígida**).

Alerta O aplicativo deseja acessar a Internet

Se você tiver selecionado a segurança **Padrão** ou **Rígida** nas opções de Configurações de segurança, o Personal Firewall exibirá um alerta (Figura 2-5) quando detectar conexões de Internet ou de rede para aplicativos novos ou modificados.

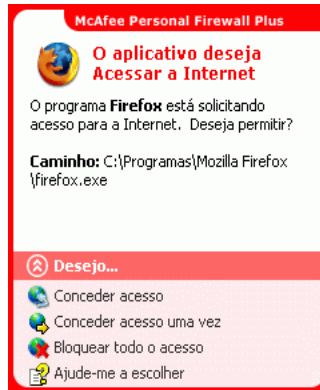



Figura 2-5. Alerta O aplicativo deseja acessar a Internet

Se for exibido um alerta recomendando cuidado ao permitir que o aplicativo acesse a Internet, clique em **Clique aqui para obter mais informações** para obter mais informações sobre o aplicativo. Essa opção será exibida no alerta somente se o Personal Firewall estiver configurado para usar recomendações inteligentes.

A McAfee talvez não reconheça o aplicativo que está tentando obter acesso à Internet (Figura 2-6).

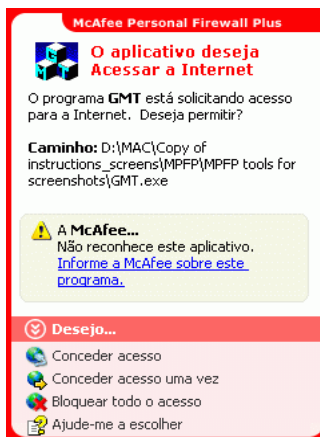



Figura 2-6. Alerta Aplicativo não reconhecido

Portanto, a McAfee não pode fornecer nenhuma recomendação sobre como lidar com o aplicativo. É possível relatar o aplicativo à McAfee clicando em **Informe a McAfee sobre este programa**. Uma página da Web será exibida solicitando informações relacionadas ao aplicativo. Forneça o máximo de informações que souber.

As informações enviadas são usadas juntamente com outras ferramentas de pesquisa pelos operadores do HackerWatch para determinar se um aplicativo merece estar relacionado em nosso banco de dados de aplicativos conhecidos e, em caso afirmativo, como ele deve ser tratado pelo Personal Firewall.

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Conceder acesso** para permitir ao aplicativo uma conexão de entrada e saída da Internet.
- Clique em **Conceder acesso uma vez** para conceder ao aplicativo uma conexão temporária à Internet. O acesso é limitado ao tempo decorrido entre a inicialização e o encerramento do aplicativo.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.
- Clique em **Conceder acesso de saída** para permitir uma conexão de saída (segurança **Rígida**).
- Clique em **Ajude-me a escolher** para exibir a Ajuda on-line sobre as permissões de acesso do aplicativo.

Alerta O aplicativo foi modificado

Se você tiver selecionado a segurança **Confiável**, **Padrão** ou **Rígida** nas opções de Configurações de segurança, o Personal Firewall exibirá um alerta (Figura 2-7) quando o Personal Firewall detectar a alteração de um aplicativo ao qual havia sido permitido o acesso à Internet. Se você não tiver atualizado este aplicativo recentemente, tome cuidado ao permitir o acesso deste aplicativo à Internet.

Figura 2-7. Alerta O aplicativo foi modificado

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Conceder acesso** para permitir ao aplicativo uma conexão de entrada e saída da Internet.
- Clique em **Conceder acesso uma vez** para conceder ao aplicativo uma conexão temporária à Internet. O acesso é limitado ao tempo decorrido entre a inicialização e o encerramento do aplicativo.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.
- Clique em **Conceder acesso de saída** para permitir uma conexão de saída (segurança **Rígida**).
- Clique em **Ajude-me a escolher** para exibir a Ajuda on-line sobre as permissões de acesso do aplicativo.

Alerta O aplicativo solicita acesso como servidor

Se você tiver selecionado a segurança **Rígida** nas opções de Configurações de segurança, o Personal Firewall exibirá um alerta (Figura 2-8) quando detectar que um aplicativo ao qual você concedeu acesso à Internet solicitou acesso como servidor.

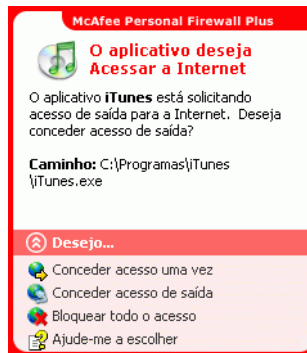



Figura 2-8. Alerta O aplicativo solicita acesso como servidor

Por exemplo, um alerta é exibido quando o MSN Messenger solicita acesso como servidor para enviar um arquivo durante um bate-papo.

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Conceder acesso uma vez** para permitir ao aplicativo um acesso temporário à Internet. O acesso é limitado ao tempo decorrido entre a inicialização e o encerramento do aplicativo.
- Clique em **Conceder acesso como servidor** para permitir ao aplicativo uma conexão de entrada e saída da Internet.

- Clique em **Restringir ao acesso de saída** para proibir uma conexão de entrada da Internet.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.
- Clique em **Ajude-me a escolher** para exibir a Ajuda on-line sobre os alertas verdes de permissões de acesso do aplicativo.

Alertas verdes

Os alertas verdes notificam sobre os eventos no Personal Firewall, como aplicativos que receberam acesso à Internet automaticamente.

Programa com permissão para acessar a Internet — esse alerta é exibido quando o Personal Firewall concede acesso à Internet automaticamente a todos os aplicativos novos e, em seguida, o notifica (segurança **Confiável**). Um exemplo de aplicativo modificado é um aplicativo com regras modificadas para permitir automaticamente o acesso do aplicativo à Internet.

Alerta Aplicativo com permissão para acessar a Internet

Se você tiver selecionado a segurança **Confiável** nas opções de Configurações de segurança, o Personal Firewall concederá automaticamente acesso à Internet para todos os aplicativos novos e o notificará com um alerta (Figura 2-9).

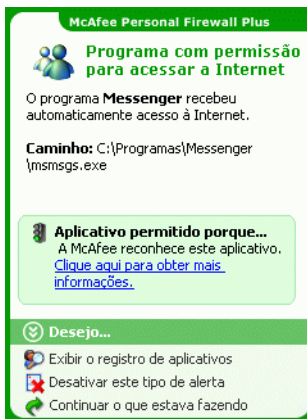



Figura 2-9. Programa com permissão para acessar a Internet

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Exibir o registro de aplicativos** para obter detalhes sobre o evento através do registro Aplicativos da Internet (consulte *Sobre a página Aplicativos da Internet* na página 20 para obter detalhes).
- Clique em **Desativar este tipo de alerta** para impedir que esse tipo de alerta seja exibido.

- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.

Alerta O aplicativo foi modificado

Se você tiver selecionado a segurança **Confiável** nas opções de Configurações de segurança, o Personal Firewall concederá automaticamente acesso à Internet a todos os aplicativos modificados. Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Exibir o registro de aplicativos** para obter detalhes sobre o evento através do registro Aplicativos da Internet (consulte *Sobre a página Aplicativos da Internet* na página 20 para obter detalhes).
- Clique em **Desativar este tipo de alerta** para impedir que esse tipo de alerta seja exibido.
- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.
- Clique em **Bloquear todo o acesso** para proibir uma conexão à Internet.

Alertas azuis

Os alertas azuis contêm informações que não exigem respostas.

- **Tentativa de conexão bloqueada —** esse alerta é exibido quando o Personal Firewall bloqueia o tráfego não desejado de rede ou de Internet (Segurança padrão, rígida ou confiável).

Alerta Tentativa de conexão bloqueada

Se você tiver selecionado a segurança **Confiável**, **Padrão** ou **Rígida**, o Personal Firewall exibirá um alerta (Figura 2-10) quando bloquear o tráfego de rede ou de Internet não desejado.

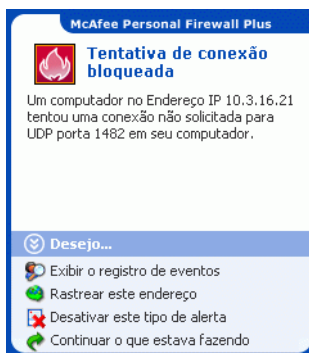



Figura 2-10. Alerta Tentativa de conexão bloqueada

Veja uma breve descrição do evento e escolha uma das opções a seguir:

- Clique em **Exibir o registro de eventos** para obter detalhes sobre o evento através do registro de Eventos de entrada do Personal Firewall (consulte *Sobre a página Eventos de entrada* na página 22 para obter detalhes).
- Clique em **Rastrear este endereço** para executar um rastreamento visual dos endereços IP deste evento.
- Clique em **Proibir este endereço** para impedir que o endereço acesse o seu computador. O endereço é adicionado à lista de endereços IP proibidos.
- Clique em **Confiar neste endereço** para permitir que o endereço IP acesse o seu computador.
- Clique em **Continuar o que eu estava fazendo** se não desejar executar nenhuma ação além do que o Personal Firewall já tenha feito.

Índice

P

R

T

W